Chapter 3: Grid Certificates

3.1 About Grid Certificates

Grid user authentication (discussed in section 2.1 *What is a VO?*) is based on grid certificates, which are analogous to Kerberos principals (familiar to Fermilab researchers!) in that they are unique identifiers for individuals. A certificate is a long-term electronic credential, remaining valid for a year, typically. A public-key X.509[1] certificate (the kind the grid community recognizes) is nothing more than a digitally signed statement from some entity (a Certificate Authority, described below), saying that some particular identifier belonging to another entity (e.g., a VO member) has some specific value.

The principal identifier that is used for this purpose is called a Distinguished Name, or DN (which adheres to the X.500 standard, in case you come across that term). It is a string that includes the individual's Common Name (CN), Organizational Unit (OU), Organization (O), Domain Component (DC), and sometimes other information, e.g.,

```
/DC=org/DC=doegrids/OU=People/CN=Joe Smith 999999
```

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be.

There are a number of Certificate Authorities. A VO must choose which CAs it will recognize, and establish an agreement with each. An agreement is required between these parties because the CA needs to know where to go or who to contact to verify the identity of each certificate applicant.

Software tools commonly in use for implementing grids (e.g., Globus tools) require that individuals submitting jobs be authenticated with a short-term authentication Grid proxy. The VOMS system creates these automatically from the users' long-term certificates (see section 2.2 *VOMS and VOX*).

[1] You may hear the terms PKI, public keys, private keys, X.509 Distinguished Name, digital signatures and so on, associated with these certificates. Defining these terms is beyond the scope of this document.

3.2 Obtaining and Loading a Grid Certificate

You must request a long-term X.509 credential from a certificate authority, e.g., the DOEGrids Certificate Service at `http://www.doegrids.org/index.html`. Instructions are provided at the CA's web site. You can request certificates from multiple CAs, if you like, as long as the VO you wish to join (or have joined) has agreements with them.

X.509 Grid proxies can be issued automatically for Fermilab users authenticated to Kerberos. See `http://computing.fnal.gov/security/pki/` for instructions. This involves downloading a KX.509[1] certificate. KX.509 can be used in place of permanent, long-term certificates. It works by creating X.509 credentials (certificate and private key) using your existing Kerberos ticket. These credentials are then used to generate the Globus proxy certificate.

You will receive your certificate in a file. You will need to load your certificate into the internet browser from which you intend to use the VOMRS, and on the same machine. Instructions for a variety of browsers can be found at `https://lcg-registrar.cern.ch/load_certificates.html`.

[1] KX.509 is described at `http://www.ncsa.uiuc.edu/~aloftus/NMI/kx509.html`.